DEPARTMENT OF STATE
PRIVACY IMPACT ASSESSMENT

Consolidated American Payroll Processing System (CAPPS)
and Interagency E-Payroll Migration

Updated April 28, 2008

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
pia@state.gov

The Department of the State
Privacy Impact Assessment for IT Projects

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any personal information about individuals or *personally identifiable information? If answer is no, please reply via e-mail to the following e-mail address: pia@state.gov. If answer is yes, please complete the survey in its entirety.

YES __X_ **NO___**

2) What is the purpose of the system/application?

The purpose of the Consolidated American Payroll Processing System (CAPPS) is to pay and process benefits for American employees as prescribed by Department of State regulations.

3) What legal authority authorizes the purchase or development of this system/application?

22 U.S.C. 2651a (Organization of the Department of State; 22 U.S.C. 3921 (Management of service); 5 U.S.C. 301 (Management of the Department of State); 22 U.S.C. 4042 (Maintenance of the Foreign Service Retirement and Disability Fund); 42 U.S.C. 653 (the Personal Responsibility and Work Opportunity Reconciliation Act of 1996); Executive Order 11491, as amended (Labor-management relations in the Federal service); 5 U.S.C. 5501-5584 (Pay Administration); and 31 U.S.C. 901-903 (Agency Chief Financial Officers).

C. DATA IN THE SYSTEM:

1) Does a Privacy Act system of records already exist?
Yes.
System Name: Personnel-Payroll Records; **Number:** State-30

2) What categories of individuals are covered in the system?
U.S. American employees and personal service contractors.

3) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The sources of the information in CAPPS are personnel and payroll records and time and attendance data. Time and attendance data is collected directly from the individuals' timesheets. Employees are also a source for the data in the system as they can change their personal information through Employee Express.

b. Why is the information not being obtained directly from the individual?

Payroll information only exists in the personnel records and can not be captured from the individual. It can only be entered by authorized Department employees, working for the Bureau of Human Resources (HR), and/or the Bureau of Resource Management (RM). Time and attendance information is submitted and approved by the employee's supervisor [reference 03 FAM], and can only be entered by authorized timekeepers.

c. What Federal agencies are providing data for use in the system?

Federal Employee Education & Assistance (FEEA); and
Office of Personnel Management (OPM)

d. What State and/or local agencies are providing data for use in the system?

None

e. From what other third party sources will data be collected?

Court orders provide garnishment information;
Long Term Care Partners, LLC provides enrollment information; and
American Foreign Service Protective Association (AFSPA) provides enrollment information and insurance benefits.

f. What information will be collected from a State Department employee and the public?

No information is collected from the public. The payroll system collects from Department employees their marital status, tax exemptions, bank information, bond information, charitable contributions information, and union dues information.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

The Office of the Legal Advisor (L) verifies the garnishment information obtained by court order. Time and attendance information from an employee is verified by the Bureau of Resource Management, Global Financial Services, Payroll Accounting Section.

b. How will data be checked for completeness?

The Bureau of Resource Management checks to make sure the information provided is complete.

c. **Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).**

The Office of the Legal Adviser and the Bureau of Resource Management ensure the data from the source is current. Employees are expected to provide current data.

d. **Are the data elements described in detail and documented? If yes, what is the name of the document?**

Yes. The data elements are described in the CAPPS Data Dictionary. A paper version of this dictionary is kept in IRM/OPS/SIO/APD. The most current version of this dictionary is kept online on the mainframe.

D. DATA CHARACTERISTICS:

1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

Yes. This data is maintained on the main frame using files, software, and JCL.

3) **Will the new data be placed in the individual's record?**

Yes

4) **Can the system make determinations about employees/public that would not be possible without the new data?**

No determinations are made about the public. As for employees, these determinations could be made using the data in the system. If an employe's data does not exist in the system, then no determinations can be made.

5) **How will the new data be verified for relevance and accuracy?**

Output reports are reviewed for accuracy by the Bureau of Resource Management

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

ACF2 provides the controls to protect the data from unauthorized access or use.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

Yes. Only employees with a "need to know" are granted access to the records. Audit trails of users on the main frame are reviewed by the ISSO and by employees' supervisors.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Yes. Many times the social security number is the personal identifier used to retrieve data. Employees can only retrieve their own personal data from Employee Express and e*Phone, both of which are protected by individual user IDs and passwords. No other personal identifiers are permissible.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

The kinds of reports produced on individuals include earnings and leave statements, accounting reports, tax reports, address reports, time and attendance data reports, and financial reports. These reports are used to review payroll operations, to send tax reports to individuals for tax filing purposes, and to be available for review by the employee. Employees have access to their own records only. Authorized payroll staff has access to all the reports.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The mainframe is operated at one site with an emergency backup at another site. Mirroring software is used to maintain consistency of the data.

2) What are the retention periods of data in this system?

56 years for pay history data and 7 years for tax data.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Reports are shredded. Data residing on physical media (tapes, disk drives) is eradicated and, when necessary, the physical media is destroyed, according to the Department's Records Disposition schedule.

4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Yes by using Report.Web and e*Phone.

5) How does the use of this technology affect public/employee privacy?

It does not in anyway affect public privacy. Sensitive But Unclassified data on employees is reflected in the reports generated by Report.Web and by e*Phone.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes. Sensitive But Unclassified data on employees is included in CAPPS.

7) What kinds of information are collected as a function of the monitoring of individuals?

Sensitive but unclassified data on employees is included in the pay history. Examples are individuals' names, social security numbers, pay information, etc.

8) What controls will be used to prevent unauthorized monitoring?

Monitoring is restricted to individuals granted access by the information system security officer (ISSO) based on the supervisor's recommendation for access level.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

N/A. This system is not being modified

11) Are there forms associated with the system? YES ___ NO _X_

F. ACCESS TO DATA:

1) Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?

Managers, system administrators, and developers have read access to the data. Authorized users have read and change access. These individuals include Payroll Service Center personnel, accounting personnel, and Bureau of Human Resource Management personnel.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes. Table-driven On-line Foundation Software (TOFS) Security Plan

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

User's access is restricted to the access granted by the supervisor and ISSO.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials.)

Preventing misuse is accomplished through several mechanisms including review of audit trails showing who used the system and for what purpose, by the software placing limits on the amount of adjustment that can be made to an individual's pay, and by the ISSO auditing any activity on the local area network. Training covering the use and misuse of Sensitive But Unclassified dat is provided yearly..

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?

Yes, contractors are involved with the operation and maintenance of the system (this project is in the operation and maintenance phase.
Yes, privacy act clauses are inserted into the contractors' contracts.
Rules of conduct have been established (this system is now 18 years old and rules of conduct were established many years ago). Yearly training is conducted by the Bureau of Diplomatic Security (DS) to remind employees of the rules of conduct when dealing with Sensitive But Unclassified information

6) Do other systems share data or have access to the data in the system? If yes, explain.

Yes. The Bureau of Human Resource Management shares data with the payroll System (Bureau of Resource Management).

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The Information System Security Officer (ISSO).

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?

No.

9) If so, how will the data be used by the other agency?

N/A based upon #8 above.

10) Who is responsible for assuring proper use of the data?

The Information System Security Officer (ISSO).